

REMARKS

Amendments

Applicant has amended the independent claims to clarify that a security preference for an access point specifies one authentication protocol from a set of authentication protocols that are supported by the access point. Applicant respectfully submits that no new matter has been added because the Specification describes two different exemplary authentication protocols that may be used by an access point in accordance with the invention (*see* page 19, lines 1-5: Open Access and Shared Key authentication protocols). Applicant further respectfully submits that the invention is not limited to access points that support only the exemplary authentication protocols.

Rejections

Rejections under 35 U.S.C. § 102(a)

Claims 1, 16, 21, 26, 31, 36, 42 and 46

Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand rejected under 35 U.S.C. § 102(a) as being anticipated by Patiyoot, et al. ("Technique for authentication protocols and key distribution on wireless ATM networks", ACM SIGOPS Operating System Review, Volume 32, Issue 4, October 1998). Patiyoot discloses using a public-private key pair authentication protocol to authenticate a wireless ATM terminal (WAT) to a wireless ATM server (WAS).

Applicant respectfully submits that the Examiner has misinterpreted the claimed term "security preference." As defined by Applicant, a security preference is one of a set of authentication protocols used by an access point. Although the Examiner is required to interpret a claim term according to its definition in the Specification, Application has amended the claims to incorporate the definition of security preference to clarify the meaning of the claims.

Patiyoot does not teach or suggest that an access point sends a security preference that is one of a set of authentication protocols supported by the access point because Patiyoot discloses that the WAS only supports a single authentication protocol.

Accordingly, Applicant respectfully submits that Patiyoot does not anticipate Applicant's invention as claimed in claims 1, 16, 21, 26, 31, 36, 42 and 46 and requests the withdrawal of the rejection of the claims under 35 U.S.C. § 102(a).

Rejections under 35 U.S.C. § 103

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis, U.S. Patent No. 6,526,506 (previously cited), in view of Quick Jr., U.S. Patent No. 6,178,506 (previously cited).

Lewis discloses an access point that uses a single authentication protocol: shared key. Quick discloses an access point (local server system) that uses a single authentication protocol: public/private key pair. Thus, the combination cannot be properly interpreted as teaching or suggesting an access point sending a security preference that is one of a set of authentication protocols supported by the access point because neither Lewis and Quick even suggest an access point that supports more than one authentication protocol.

Furthermore, the Examiner continues to assert that the rationale used to reject the method of claim 1 cover the data structure claimed in independent claim 42. However, there is no disclosure in either Lewis or Quick that even suggests the arrangement of data claimed by Applicant in claim 42.

Finally, although clearly Lewis discloses two different devices (key distribution server and access point) providing two different layers of encryption to secure a network, the Examiner has combined Lewis' key distribution server and access point into a single device to read on Applicant's claimed access point. However, using a single device contradicts Lewis' teaching that the key distribution server and the access point are separate devices because they provide different layers of encryption. In the present Office Action, the Examiner cites U.S. Patent 6,889,321 to Kung as support for his assertion that Lewis' key distribution server and the access point can be combined into a single device. The Examiner provided no rationale as to how Kung overcomes Lewis' clear teaching that the devices are separate. In fact, Kung is directed toward setting up a

peer-to-peer connection between two endpoint gateways using a key distribution server as an intermediary. As well-known in the art, a peer-to-peer connection, such as disclosed by Kung, is not equivalent to a mobile device-access point connection, such as disclosed by Lewis. Even assuming an equivalence between the two distinct types of connection, Applicant has reviewed Kung and can find no disclosure that overcomes Lewis' clear teaching that the key distribution server and the access point are different devices.

Accordingly, the combination of Lewis and Quick cannot render obvious Applicant's invention as claimed in claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51, and Applicant respectfully requests the withdrawal of the rejection of the claims under 35 U.S.C. § 103(a) over the combination.

Claims 4-8, 18, 23, 28, 33, 39, and 49

Claims 4-8, 18, 23, 28, 33, 39, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Quick, further in view of Schneier ("Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 1996). Schneier is directed toward various cryptographic processes and contains no disclosure related to access points that send a security preference as claimed in the independent claims, from which claims 4-8, 18, 23, 28, 33, 39, and 49 depend.

Accordingly, the combination of Lewis, Quick and Schneier cannot render obvious Applicant's invention as claimed in claims 4-8, 18, 23, 28, 33, 39, and 49, and Applicant respectfully requests the withdrawal of the rejection of the claims under 35 U.S.C. § 103(a) over the combination.

SUMMARY

Claims 1-51 are currently pending. In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Sue Holloway at (408) 720-8300 x309.

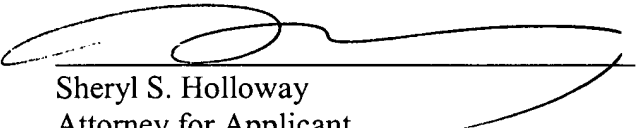
Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR
& ZAFMAN LLP

Dated: Nov. 23, 2005



Sheryl S. Holloway
Attorney for Applicant
Registration No. 37,850

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026